Мусієнко К.*

ОЦІНКА ПОТЕНЦІАЛУ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ З МЕТОЮ УПЕРЕДЖЕННЯ КІБЕРВІЙН

У результаті інформаційно-технологічної революції настала епоха глобальної мобільності інформації. Вперше в історії людства відбулося пониження статусу держави, обмеження статусної інституційної культури. Домінуючим стає пріоритет віртуальних технологій над матеріально-практичними. Статусні комунікації традиційно виступають у трьох основних формах - політичної, соціальної та географічної комунікації [1].

Політичні комунікації асоціюються з державними інститутами, наддержавами, великими державами. Інформаційна революція завдала удару по державній монополії на інформацію і веде до зниження статусу держави-нації. Вона трансформувала уявлення про національну безпеку, які протягом століть виходили з передумов створення військової та економічної потужності держави. Інформаційна революція висунула нові вимоги до проблем національної безпеки, намітилися тенденції до стирання статусних кордонів. Змінюються головні пріоритети національної безпеки. Об'єктами ураження в інформаційних війнах і конфліктах постають поряд з матеріальними цілями інформаційні ресурси [1; 2].

Соціальні комунікації асоціюються з посадою, званням і багатством. Зі століття в століття доступність інформації залежала не тільки від географічних відстаней і часу передачі, але в першу чергу від соціального статусу. Інформаційні інтернет-технології, забезпечивши доступ будь-якого користувача до світового інформаційного простору, перетворюють статусні комунікації майже в ніщо. У приватних осіб з'явився доступ до каналів зв'язку та джерел інформації, які колись мали статусну доступність [2].

Географічні комунікації визначаються місцем розташування (центр - периферія). В Інтернеті немає вигідного географічного положення. У багатовимірному комунікаційному просторі Землі на кордонах кіберпростору і реального географічного простору утворюються концентровані вузли зв'язку - кіберпорти - своєрідні вільні гавані постіндустріальної епохи. Найбільшими кіберпортами є Силіконова долина (США, Каліфорнія) і держава Сінгапур [3].

Цілком очевидно, що в сучасному світі, в якому дедалі більшу роль в житті держави, її економіці та системі безпеки, відіграють кіберпростір та сучасні інформаційні технології, не можна обійти увагою ті загрози, які пов’язані з застосуванням цих високих технологій. У цьому зв’язку все частіше можна почути такі слова, як «кібершпигунство» та «кібервійна» [3].

Під кібервійною прийнято розуміти комп'ютерне протистояння у просторі Інтернет. Передусім вона спрямована на дестабілізацію комп'ютерних систем і доступу до мережі державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країн, які покладаються на Інтернет у повсякденному житті.

З юридичного погляду проблема полягає в тому, що в міжнародному праві немає чітких критеріїв, за допомогою яких можна було б відокремити акти звичайного комп’ютер-

* студентка 3 курсу спеціальності «міжнародна інформація» Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

Науковий керівник: доц. Андрєєва О.М.

ного хуліганства від таких нападів, які завдяки своїй серйозності мають характер збройного нападу на державу, або є початком збройної агресії проти певної держави. Власне кажучи, йдеться про необхідність визначення міжнародно-правового поняття «кібервійни» [4].

На сучасному етапі міжнародні організації за участю Росії і США ведуть роботу над створенням конвенції з ведення кібервійни. Не виключено, що незабаром до кібервійн будуть застосовувати правила міжнародних конвенцій, а частина шкідливих програм міжнародне співтовариство віднесе до зброї масового ураження. Зокрема ці проблеми обговорювались на Мюнхенській конференції з безпеки [5].

Під час конференції було порушено питання про можливість застосування нинішніх правил ведення воєн в реальному світі для кіберпростору. Правила ведення військових дій описані у двох міжнародних конвенціях: Гаазькій (1899 і 1907 р.р.) і Женевській (1929).

Дослідження про застосування конвенцій під часи кібервійн створено двома співавторами: головою технологічного напрямку Інституту «Схід-Захід» Карлом Раушером і Андрієм Коротковим, завідуючим кафедри глобальних інформаційних процесів і ресурсів МДІМВ [5; 6].

В документі пропонують розглянути можливість використання спеціальних маркерів для вказівки захищених зон в кіберпросторі, подібно до того, як Червоний хрест позначає що перебувають під його захистом транспортні засоби та інші матеріальні об'єкти.

Крім того, міжнародним органам належить вирішити, чи є кібернетична зброя (віруси, черв'яки, трояни) аналогом видів озброєнь, заборонених Женевським протоколом (наприклад, отруйних газів) [7].

Можливо, найцікавіше запитання, яке порушено у доповіді, полягає в тому, як витлумачити принципи міждержавних конвенцій, в той час, як учасники кіберконфліктів не є суб'єктами держави.

Додатково ускладнює застосування старих міждержавних договорів той факт, що географічним джерелом кібератаки, як правило не є саме потенційно зацікавлена держава.

Навіть за наявності військових конвенцій у реальному світі, їх положення постійно порушуються. Однак, треба пам'ятати, що такі порушення призводять до виникнення міжнародних трибуналів: Нюрнберзького і Гаазькому. Не виключено, що ухвалення нового документу призведе до створення уповноваженого органу, який мав би право судити хакерів.

Отже, кібербезпека все більше стає реальністю на національному рівні. Проте створення по-справжньому ефективної системи кібербезпеки не можна уявити без відповідних дій на міжнародному, світовому рівні. Саме тут особливу роль має відіграти міжнародне право і міжнародні структури.

Список використаних джерел

1. Експерти хочуть встановити правила ведення кібервійни [Електронний ресурс]: Інтернет-портал «Центр Інформаційної Безпеки»– Режим доступу до матеріалу: http://www.bezpeka.com/ua/news/2011/02/08/cyberwar-rules-to-be-set.html
2. The threat from the internet: Cyberwar [Електронний ресурс]: Інтернет-портал «The Economist» – Режим доступу до матеріалу: http://www.economist.com/node/16481504?story_id=16481504&source=features_box1
3. Западные СМИ: Кибероружие страшне, чем ядерное [Електронний ресурс]: Інтернет-портал «Росблат»– Режим доступу до матеріалу: http://www.rosbalt.ru/2010/10/05/777929.html

4. Поможет ли государство победить в кибервойне? [Електронний ресурс]: Інтернет-портал «PSweek» – Режим доступу до матеріалу: http://www.pcweek.ru/security/article/detail.php?ID=128686
5. Россия и США пишут правила кибервойны [Електронний ресурс]: Інтернет-портал «CNews» – Режим доступу до матеріалу: http://safe.cnews.ru/news/top/index.shtml?2011/02/04/426037
6. Мережко О. Проблеми кібервійни та кібербезпеки в міжнародному праві [Електронний ресурс]: Інтернет-портал «Юстиніан» – Режим доступу до матеріалу: http://www.justinian.com.ua/article.php?id=3233
7. Первая кибервойна началась [Електронний ресурс]: Інтернет-портал «trust.ua» – Режим доступу до матеріалу: http://www.trust.ua/news/36960.html